International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT217233

Revelation of Cryptography

Soham Mehta, Deep Nandu
Department of Computer Engineering, SAKEC, Mumbai, Maharastra, India

Article Info
Volume 7, Issue 2
Page Number : 108-117

Publication Issue :
March-April-2021

Article History
Accepted : 25 March 2021
Published : 31 March 2021

ABSTRACT

As the means of communications matured and developed so did the need of secret message keeping, as we discover new and more sophisticated cryptographic techniques are being developed to aid in securing the communications between sender and receiver. Some of cryptographers started to come up with new techniques to hide the data using new encryption methods while others came up with new techniques to break the said encryption methods and this led to many great evolutions in the communication sector, as the communications became digital from analog secret message keeping became far more important and led to the introduction of various protocols and frameworks to support their need of secret message keeping.

Keywords: Cipher text, Encryption, Secret Message, Cryptographic Techniques, Secret Message, Cryptanalysis, Modern Encryption

I. INTRODUCTION

Cryptography is the science of writing codes and ciphers for secure communication, which is one of the most important elements that goes into making modern communication, networks, cryptocurrencies, and blockchains possible. The cryptographic techniques used today, however, are the result of a long history of development. Since ancient era, people have used cryptography to transmit information in a secure manner. The modern Cryptography is a result of seesaw battle between code makers and code breakers that has pushed the very boundaries of science. Following is the fascinating history of cryptography that has led up to the advanced and sophisticated methods used for modern digital encryption. But before that lets understand few of the terms related to cryptography:

Plain text: Refers to text that can be read by a normal person.
Cipher text: Refers to encrypted text that might be gibberish for a normal person.
Key: Refers to a number or a word that can be used to encrypt or decrypt the plain text
Shifts: Refers to replacing each letter in the message by a letter that is some fixed number of positions further along in the alphabet list.
Encryption: The conversion of plain text to cipher text.
Decryption: The conversion of cipher text to plain text
Cryptanalysis: The study of cipher text and cryptosystems
Cryptanalyst: The agent (human/computer) that performs cryptanalysis.

The art of secret writing aka cryptography was developed along with the art of writing. As the

humans evolved and became civilized so did the need of secure means of communication, humans got organized in tribes or groups, and later kingdoms which brought idea or problems such as power, battles, supremacy, and politics. These ideas further fuelled the natural need of people to communicate secretly with selective recipient which in turn ensured the continuous evolution of cryptography as well.

In the current generation of information age encryption plays a major role in data transmission, from metadata to information everything transmitter over a network is highly encrypted to maintain the data integrity and to avoid the data from being leaked or getting misused.

II. ROOTS OF CRYPTOGRAPHY

Cryptography is as ancient as the art of writing, early civilizations seemed to have used cryptography to some degree where symbol replacement appears in both ancient Egyptian and Mesopotamian writings. Since prehistoric age encryption is used by civilization to protect the data or messages that needs to be kept away from the prying eyes, one of the oldest examples of encryption techniques hieroglyph being 4000 years old used by the ancient Egyptian to keeps records or to pass message that were known only by the '*Scribes*'. The very first technique of cryptography that can be traced is through the history is Hieroglyph. It is the oldest cryptographic technique and was used by the Egyptians around 4000 years ago. The Hieroglyph was found on the tomb of an Egyptian noble named Khnumhotep II, who lived approximately 3,900 years ago. The scribe who drew the symbols on his master's tomb was drawing his master's life on the tomb, but instead of using standard numbers and symbols he used unusual signs and symbols to obscure the meaning of the inscriptions. The only explanation that could be found is that Egyptian scribes wanted to give formal appearance to their writings. Hieroglyph was also a code that was only known to the scribes could use and who could send the message on behalf of the king they used it as an opportunity to use their formal language skills to impress the king.

Figure 1: Egyptian Symbols used 4000 years ago

Figure 2: Symbols on tomb of Khnumhotep II

By later era of relics and artifacts, cryptography was largely used to protect classified and or important military information, a purpose that it serves till this day. A good example for the early forms of cryptography would be from the Greek city – State of Sparta around 500 BCE, the Spartans who were trying to send secure message to their military campaigns they used a tool called scytale. Scytale consisted of a cylinder with a piece of parchment around it on which the message was written. The parchment is wrapped around cylinder and the message is written on it. This tool performed the transposition cipher on the message. The receiver uses the rod of the same diameter on which the parchment is wrapped to read the message.

Figure 3: S Scytale Example

Possibly the most advance cryptographic system in the ancient civilization was established by the Romans, one of the most famous and prominent examples would be *Caesar Cipher*, around 5th century AD Julius Caesar a Roman general commander in the Roman Army developed a cipher or encryption technique that is one of the widely known encryption techniques which is called Caesar cipher. Caesar is also known as the shift cipher it is like the substitution where the letters in the plain text are replaced by the letters that are some fixed positions down the alphabet. The Caesar cipher provided reasonably secure means of communication; apart from the encryption of the message, the reason is that the enemies of the Roman Empire could not have understood since to them it would have been a foreign language.

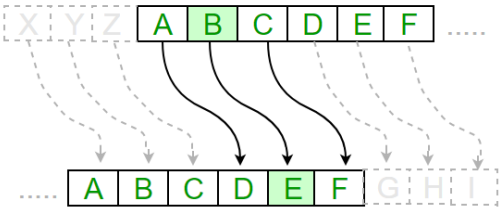


Figure 4: Substitution Cipher

Around 900AD another civilization rising in the east, Arab society was one the most literate cultures in the world and the study of code flourished, the Arabs were the first to record the method of *transposition* the scrambling of letters as well as *substitution* the replacement of letters with numbers and symbols they were the first to outline specific techniques of code breaking that involved *mathematical or frequency analysis* and were the first to suggest the most frequent coded letter represents the most frequent plain text.

III. Middle Ages and Renaissance

With the Renaissance cryptology has a rebirth in Europe in 1466 an Italian architect developed a greatest Cryptologic invention in a thousand year at the urging of the Vatican, it was a system of rotating cipher disks with two rings of letters and several numbers by scrambling so many letters randomly, one is the alphabet in which the original message is written, while the second is an entirely different alphabet in which the message appears after being encoded. In polyalphabetic cipher two same letter in the plain text might get encrypted into two different letters, even the length of the plain text and cipher text might be changed in the polyalphabetic cipher if the plain text consists of 5 letters the cipher text might have 10 letters. Combined with the traditional ciphers. Polyalphabetic ciphers increased the security of the message greatly. It became the first to challenge the Arab code breaking method of frequency analysis which was later called *Polyalphabetic Substitution* earlier known as *Alberti system* and it became the base to many modern cipher systems.

A French Diplomat improved the Alberti system in 1586 by creating a cipher style that later came to be known as *Vigenere cipher*. Vigenere cipher uses the grid of letter that gives the method of substitution the grid is known as Vigenere cipher or Vigenere table made up of 26 letters offset from each other by one letter. The key exception of Vigenere cipher from the Caesar cipher is that the key of the Vigenere changes throughout the process and in the Caesar cipher the key remains the same for entire process.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Figure 5: Vigenère Cipher Table

But the real revolution in cryptography was just ahead, telegraph made it possible to send message at long distance possible which raised the necessity for cryptology, in 1844 with the invention of *Morse Code* a series of dots and dashes to communicate over the telegraph and since the code was public and messages could be easily intercepted the need for new secret codes became acute.

IV. Modern Age

With the dawn of 20th century an Italian physicist changed the world of code with the invention of radio the messages needed to be out into code which led to the great growth of codes and ciphers, radio messages were enciphered and sent in Morse code across the airways but also has constant and massive stream of intercepts to the enemy, with the start of World war 1 the need of new ciphers and code breakers escalated.

A. Era of War - World War I's influence on cryptography

a. Zimmermann Telegram

In 1917, at the height of WW1, the British cryptographers come across an encoded German telegram, which is now known as the *Zimmermann Telegram*. The British were able to decipher the telegram which changed the tides of war and became one of the important events in WW1. During the start of WW1, the United States had decided to remain neutral. The telegram was sent in response of the conflict British naval blockade, Germany broke the pledge to curb the submarine warfare by firing missiles at a civilian ship. Germany broke the Sussex pledge after which the United States severed all diplomatic ties with the Germany. Germany feared that United States might join the war and join the allies, hence few weeks later British found the Zimmermann telegram which was written by German foreign minister Arthur Zimmermann to the German minister to Mexico, Heinrich von Eckhardt, offering United States territory to Mexico in return for joining Germany as their ally in the WW1. The British deciphered the message and on February 24th they presented and helped draw United State into war and in April 1917 the United States formally declared war on Germany and its allies.

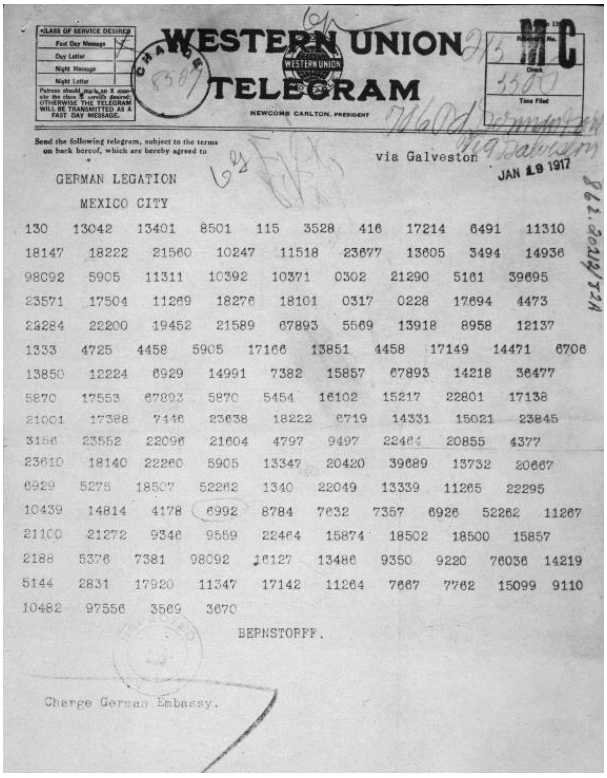
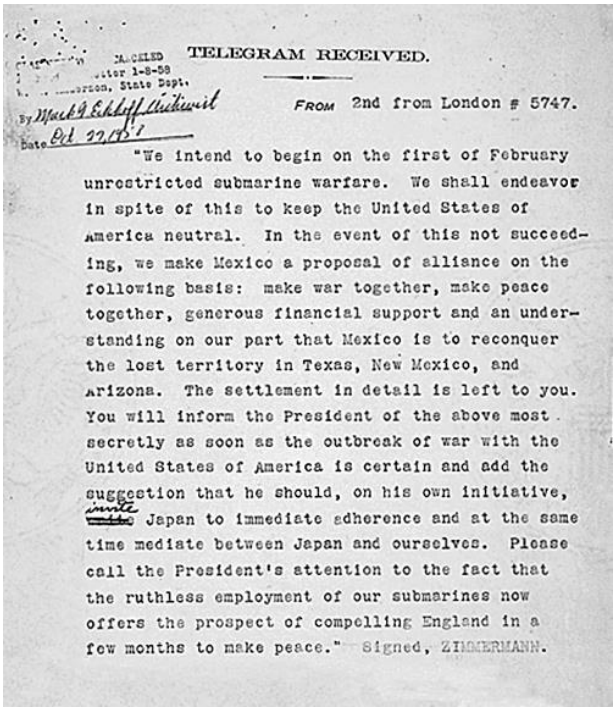

WESTERN UNION
TELEGRAM
NEWCOMB CARLTON, PRESIDENT
via Galveston
JAN 19 1917
GERMAN LEGATION
MEXICO CITY
130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
23284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7446 23638 18222 6719 14331 15021 23845
3156 23552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3670
BERNSTORFF.
Chrge German Embassy.

Figure 6: Encoded Zimmerman Telegram



TELEGRAM RECEIVED.

FROM 2nd from London # 5747.

"We intend to begin on the first of February unrestricted submarine warfare. We shall endeavor in spite of this to keep the United States of America neutral. In the event of this not succeeding, we make Mexico a proposal of alliance on the following basis: make war together, make peace together, generous financial support and an understanding on our part that Mexico is to reconquer the lost territory in Texas, New Mexico, and Arizona. The settlement in detail is left to you. You will inform the President of the above most secretly as soon as the outbreak of war with the United States of America is certain and add the suggestion that he should, on his own initiative, invite Japan to immediate adherence and at the same time mediate between Japan and ourselves. Please call the President's attention to the fact that the ruthless employment of our submarines now offers the prospect of compelling England in a few months to make peace." Signed, ZIMMERMANN.

Figure 7: Decoded Zimmerman Telegram

b. Choctaw Code talkers

The Choctaw are the Native American people who originally occupied the now South-eastern United States. The Choctaw code talkers were the group of Choctaw Indians from Oklahoma who invented a system where they used the Native American languages as military codes. During the WW1 period, the United States was facing a lot of problems with the lack of secure communication, the phone calls made were all intercepted by the Germans revealing all the moves and strategies made by the allies. During this period, an American officer Colonel Alfred Wainwright Bloor, notices two American Indians serving in the 142nd infantry and observed that he could not understand them and assumed that no matter how good the Germans were with their English they will not be able to understand this. Besides many of these Native American languages did not have any written form. Colonel Bloor decided to use this cipher in the field and deployed the code, he deployed a regular message in place of a military message and Choctaw code talkers proved to be successful. The next time the system was deployed in a military mission which was a particularly important event for the allies and to enemy's complete surprise the Germans were not able to understand the conversation and could not decrypt the message. This turned the tide of the war and by placing the Choctaw Code talkers in every battalion and company the allies were able to communicate without hesitation of the conversation being overheard.

B. Era of War - World War II's influence on cryptography

a. Rivalry of Enigma and Bombe:

World war II brought on creation of new and revolutionary techniques in field of encryption by push cryptanalyst and cryptographers to their limits and leading to inventions of infamous Enigma Machine and The Bombe Machine that revolutionized the technique of message passing and encryption.

By the end of World war 1, a German Electrical Engineer invented the Enigma, an electromechanical device that was used by the Germans to encode and decode their secret messages. The machine is made up of multiple parts including a keyboard, a lamp board, rotors, and internal electronic circuitry. Some machines, such as the ones used by the military, had an additional feature such as a plugboard that allowed approx. 10114 possible configurations, because of this many configurations the Enigma became virtually unbreakable with basic brute force methods.

During the world war to the Enigma Machine came to fame and was largely used by them to for keeping their messages a secret. Enigma's statistical security made the Nazi Germany overconfident of their abilities of secret message keeping technique which led to the downfall of the Enigma. On top of multiple errors by German Operators, the Enigma itself had several built-in weaknesses that led cryptographers to

exploit Enigma. This allowed the Allied cryptographers to decrypt a vast number of ciphered messages sent by Nazi Germans.

Alan Turing an English Mathematician and Gordon Welchman an British-American Mathematician designed an art of machine called the Bombe Machine that used electric circuitry to solve an Enigma encoded message in less than 20 minutes. The Bombe machine would try to determine the settings of the rotors and the plugboard of the Enigma machine used to send a given coded message. The standard British Bombe machine was essentially 36 Enigma machines wired together, this way, the Bombe machine would simulate several Enigma machines at once. Most Enigma machines had three rotors and to represent this in the Bombe, each of the Enigma simulators in the Bombe had three drums, one for each rotor. At each position of the drums, the configuration would be tested to see if the configuration led to a logical contradiction, ruling out that setting. If the test did not lead to a contradiction, the machine would stop and the decoder would note that configuration as a candidate solution. Then, the machine is restarted and more configurations are tested. These tests would narrow down the list of possible configurations and the candidate solutions would be tested further to eliminate ones that wouldn't work. There were usually many unsuccessful candidate solutions before the correct one was found. This machine led to breaking many of the Nazi German messages and led to the downfall of the Nazi forces.

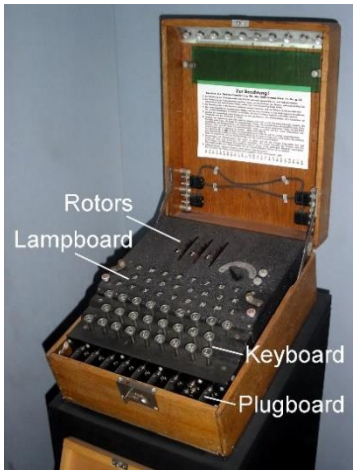


Figure 8: Enigma encryption machine used by Nazi Germany.

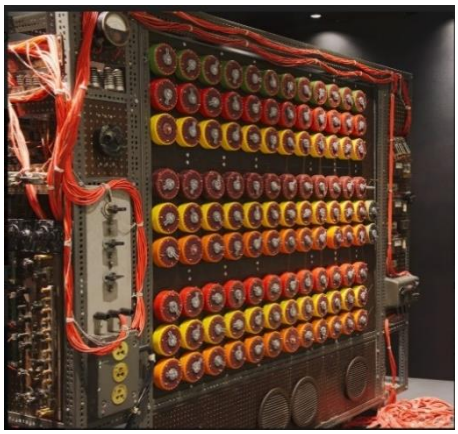


Figure 9: Bombe Machine created by the Alan Turing to break the Enigma encryption machine used by Nazi Germany.

b. Purple

While the cryptographers were busy dealing with the German Enigma, the Japanese developed a machine called *Type B Cipher Machine*, codenamed *Purple* by the US. In contrast to the Enigma's rotors, Purple was made with stepping switches commonly used for routing telephone signals. By the end of war Japanese destroyed most of these machines and were so good at keeping their encryption methods secret the US cryptographers had a hard time decrypting their messages. All the Japanese message were coded, the 26 letters of English Alphabet were divided with help of a Plug board into two groups, of 6 and respectively. The alphabets in the sixes group were scrambled using 6x25 substitution table and the letters in the

twenties group on plug board would be scrambled using 3 successive 20x25 substitution table. It was made up of an input typewriter, input plugboard, stepping switches with 6 layers to select out one of 25 permutations of the letters in 6 group, 3 stages of stepping switch each stage is a 20-layer switch with 25 output on each layer and each selected one out of 25 permutations of the alphabets, an output plug board that reversed the input and the output typewriter.

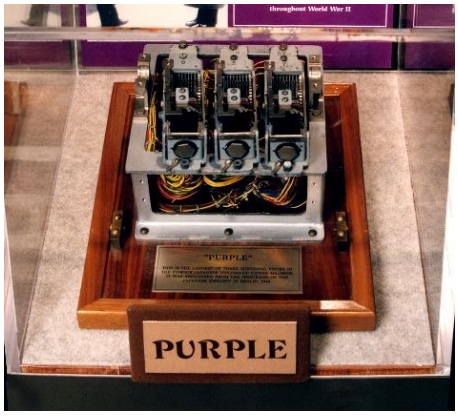


Figure 10: Purple encryption machine used by Japanese during WWII.

V. Rise of Modern Encryption

A. One - Time Pad

In the early 1900's one of the most important invention was made in the early "One –Pad Time" which is since then proven unbreakable, the one-time pad algorithm is derived from a previous cipher called Vernam Cipher that mixed the message with a key read from a paper tape or pad. The Vernam Cipher was breakable until Joseph Mauborgne recognized that if the key was random the difficulty to break the cipher would be equivalent to trying each and every possible key. Even while trying every possible key for deciphering one would need to review each and every attempt of deciphering to check if the correct key was used, the unbreakable characteristic of the one-time pad come by 2 assumptions: The key being used is completely random, also The Key cannot be used more than once. The security of one-time pad depends completely on keeping the key 100% safe. One time pad's implementation is by using XOR to fuse the plaintext with the key and creating the ciphertext and applying the same to ciphertext to produce the plaintext.

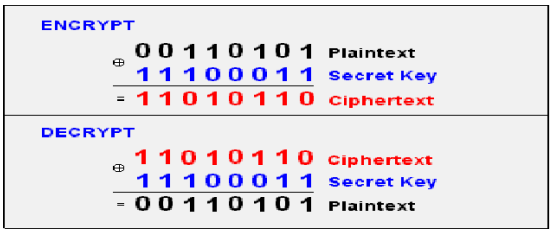


Figure 11: Example of One-Time Pad

B. Symmetric Encryption:

From all the we have understood till now any mode or method of encryption required a special secret key which needed to be secretly and securely established. This is what Symmetric Encryption is all about, symmetric key aka public key which was used to enciphering and deciphering the text, and the only means of protecting the text is by keeping the key secret, if any unintentional person obtains access to the key, the person will have full access to what is being secured by the lock.

There are many methods of implementing the symmetric cipher out of which two main methods are Stream Cipher where a stream of random or pseudo random numbers are mixed with the original message, and Block cipher which takes in a set of bits of plain texts as input and outputs similar sized block of cipher text. Some of the famous example of stream ciphers are LFSR and RC4, and for examples of block ciphers are DES and AES.

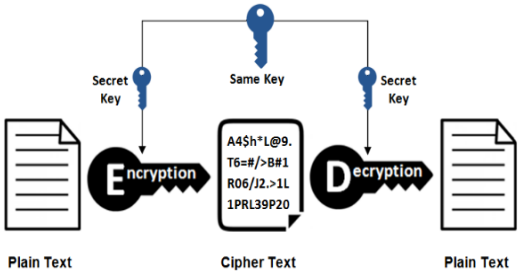


Figure 12: Symmetric Encryption

VI. Evolution of Encryption

A. Asymmetric Encryption:

During the 1970's world saw a rise of digital world which meant a new type for an encryption system was needed for the evolution of the digital world, Cryptographers and Cryptanalyst of that generation realized that if they want to send a message securely without meeting with the receiver, they would need a system that will use a different key for encryption and for decryption. But the main problem still was how to exchange the key, the key exchange problem portrays ways to exchange the keys and other information needed for establishing a secure channel for communication.

Asymmetric encryption uses a 2-key methodology consisting of a Public key and a Private key, and it depends on the type of cryptographic algorithm which key needed to be used for encryption and which to be used for decryption one way to do it was public key can be shared over non secure or public paths and the private key is only available to its owner.

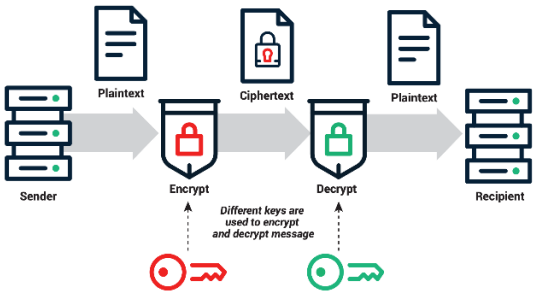


Figure 13: Asymmetric Encryption

One of the famous examples of such algorithm is Diffie – Hellman key exchange protocol published by Whitfield Diffie and Martin Hellman in 1976, this protocol allows the user to securely the secret key even if the channels are being monitored, but authentication was important when an opponent can possibly alter and monitor the message within the communication, PKI or Public Key Infrastructures were suggested as a way around this problem to authenticate the identity of the sender, where each user applies to a *Certification Authority* (CA) which is usually trusted by all parties to obtain a digital certificate which is used by a user as alterable or tamperable means for authenticating once identity.

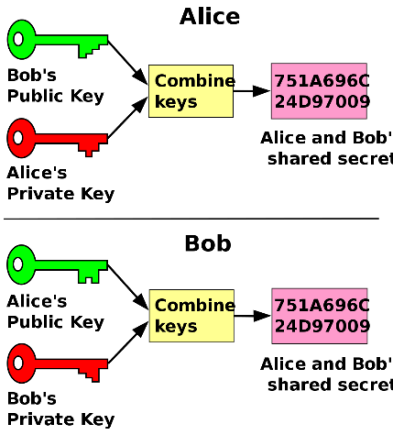


Figure 14: Diffie-Hellman Key Exchange protocol

B. RSA Encryption:

After noticing the incapability of Diffie Hellman Key Exchange to send a secret message Ron Rivest, Adi Shamir and Leonard Adleman developed a similar system to D-H protocol with a change that the message could be embedded and transmitted. RSA relies on multiplication and exponential which is way faster than prime factorization. The protocol is designed from two large prime numbers which are manipulated to give a public key and private key which can be used more than once after they are generated, a user and sender usually shares their public key which each other and keeps the private key a secret and the sender encrypts the message using users public key their own private key which user later decrypts using the secret personal private key. one of the numbers generated which is used by the RSA algorithm is the product of two large primes called modulus, in order to crack RSA attacker must calculate the prime factorization of the modulus, which results in the two primes. The strength of RSA

encryption algorithm relies on the difficultly to produce this prime factorization. RSA Encryption is the most widely used asymmetric key encryption system used for electronic commerce protocols.

VII. CONCLUSION

As the time passed the cryptographic techniques started getting more and more sophisticated, which led to more secure communication between sender and receiver, a history of more than 6000 years and yet one of the most challenging topics in the human history the helped create security, end wars and maintained the confidentially throughout the ages.

VIII. REFERENCES

[1]. Nicholas G. McDonald, Department of Electrical and Computer Engineering, University of Utah. "Past, Present, Future Methods of Cryptography and Data Encryption", Utah, USA.

[2]. Soumitra Bhattacharya. 2019. International Journal on Cryptography and Information Security (IJCIS), Vol. 9, No.1/2, June 2019,

[3]. CRYPTOLOGY AND INFORMATION SECURITY - PAST, PRESENT, AND FUTURE ROLE IN SOCIETY Whitefield Diffie, Cryptography: Past, present and Future. Springer.

[4]. https://www.tutorialspoint.com/cryptography/modern_cryptography.html

[5]. https://www.semanticscholar.org/paper/Essay-15-Cryptography-Abrams-Podell/62a3f959c11b8209f191592216d74f67beba9ffd

[6]. https://www.tutorialspoint.com/cryptography/origin_of_cryptography.html

[7]. http://www.rsa.com/rsalabs/node.asp?id=2094

[8]. Dan Boneh. The Theory and Application of Cryptology and Information Security. "Pairing-Based Cryptography: Past, Present, and Future".

[9]. https://economictimes.indiatimes.com/definition/cryptography

[10]. https://www.csoonline.com/article/3583976/what-is-cryptography-how-algorithms-keep-information-secret-and-safe.html

[11]. https://medium.com/@.Qubit/what-is-cryptography-a18423c82e47

[12]. https://towardsdatascience.com/the-basics-of-cryptography-80c7906ba2f7

[13]. http://cryptogramma.com/cryptogramma/How_it_works.html

[14]. https://www.dcode.fr/caesar-cipher

[15]. https://crypto.interactive-maths.com/vigenegravere-cipher.html

[16]. https://www.sciencedirect.com/topics/computer-science/jefferson-diskJason Andress. Science Direct. The Basics of Information Security, 2011.

[17]. https://www.sciencedirect.com/topics/computer-science/jefferson-diskEric Conrad, Joshua Feldman. Science Direct in CISSP Study Guide (Third Edition), 2016.

[18]. https://www.theworldwar.org/learn/wwi/zimmermann-telegram

[19]. https://www.choctawnation.com/history-culture/people/code-talkers

[20]. https://www.bbc.com/news/magazine-26963624

[21]. https://www.britannica.com/topic/Enigma-German-code-device

[22]. https://www.theguardian.com/technology/2014/nov/14/how-did-enigma-machine-work-imitation-game

[23]. Peter Smirnoff , Dawn M. Turner. CRYPTOMAThIC. Symmetric Key Encryption - why, where and how it's used in banking.

[24]. https://www.thesslstore.com/blog/symmetric-encryption-101-definition-how-it-works-when-its-used/ vs-asymmetric-encryption

Cite this article as:

Soham Mehta, Deep Nandu, "Revelation of Cryptography", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN: 2456-3307, Volume 7 Issue 2, pp. 108-117, March-April 2021. Available at
doi: https://doi.org/10.32628/CSEIT217233
Journal URL: https://ijsrcseit.com/CSEIT217233